THE EQUIVALENCE PROBLEM OVER FINITE RINGS

CSABA SZABÓ AND VERA VÉRTESI

Abstract. We investigate the computational complexity of deciding whether or not a given polynomial is identically 0 over a finite ring. It is proved that if the polynomial is presented as a sum of monomials, then the complexity depends only on the factor by the Jacobson-radical; it belongs to P if the factor is commutative, and coNP-complete otherwise.

1. Introduction

A *ring* is a set equipped with three operations; the multiplication $\cdot$, the addition $+$ and the additive inverse operation $-$. A *term* over a ring is an expression $t(x_1, \dots, x_n)$ built up from variables and the fundamental operation symbols in the usual manner. A term $t(x_1, \dots, x_n)$ over any ring R defines a so called *term-function* $t^R : R^n \to R$. A ring R *satisfies* an equation $s(\vec{x}) \approx t(\vec{x})$ or $R \models s \approx t$ if the corresponding term-functions s^R and t^R are the same functions. Note that terms over a ring are polynomials with integer coefficients.

The *(term) equivalence problem* for a ring R is the problem of deciding which equations are satisfied by R. Over a given ring R the instance of the equivalence problem is an equation $s(\vec{x}) \approx t(\vec{x})$, and the question is whether or not it is satisfied by R. If $s(\vec{x}) \not\approx t(\vec{x})$, then there is a substitution over R where the two term-functions s^R and t^R do not agree, so the equivalence problem is in coNP. Several times we refer to the equivalence problem as the word problem. This latter expression is used in the literature in several contexts. We use it for the equivalence problem.

Early investigations into the equivalence problem for various finite algebraic structures were carried out by computer scientists at Syracuse University where the terminology the *term equivalence problem* was introduced. In particular they considered finite commutative rings and finite lattices. In the early 1990s it was shown by Hunt and Stearns [5] that for a commutative ring R the equivalence problem is in P if

Date: April 22, 2008.

Key words and phrases. term, equivalence problem, ring, complexity.

R is nilpotent and coNP-complete otherwise. Burris and Lawrence [1] proved that the same holds for rings in general.

The formal definitions of terms and polynomials allow us to use iterated addition and multiplication, for example the expression $(x_1 + y_1)(x_2 + y_2) \cdots (x_n + y_n)$ is a term over a ring. If we expand this term into a sum of monomials, we obtain a sum of 2^n many monomials of length n. The length of a term is crucial from the computational point of view. Moreover, when a ring-term is presented, in most cases it is given as a sum of monomials. If one restricts the terms that are allowed as instances of the equivalence problem to, for example, monomials or sums of monomials, then the complexity of the problem can change. And, indeed, the complexity of the problem changes: as it is shown by Lawrence and Willard [6]; If $J(R)$ denotes the Jacobson radical of the ring R, then the equivalence problem in R for sum of monomials is in P if $R/J(R)$ is commutative.

This is the reason why Lawrence and Willard introduced the $_\Sigma$ version of the identity checking problem for rings. In the following we investigate a version of the equivalence problem where the instance terms must be given as sums of monomials. Of course every term over a ring can be written in such a form, but, as we saw, during the expansion its length can grow exponentially.

As we shall see, in most cases the multiplicative semigroup of a ring guarantees the hardness of the word problem for the ring itself. It means that to decide whether or not two monomials are equivalent is already coNP-complete for several rings. Hence hardness of the word problem for semigroups implies the hardness of the word problem for rings.

The main result of the paper is the following:

Theorem 1. *Let R be a finite ring, and let $J(R)$ denote its Jacobson-radical, then*

1. *If $R/J(R)$ is commutative, then the equivalence problem for sum of monomials is in P;*
2. *The equivalence problem for sum of monomials is coNP-complete, otherwise.*

For matrix rings the complexity of this version of the equivalence problem is already known; the equivalence problem for sum of monomials is in P, if the matrix ring is commutative and coNP-complete otherwise. This result was shown by Lawrence and Willard [6] for matrix rings whose group of units form non-solvable groups, and by Szabó and Vértesi [9, 8] for the remaining cases, $M_2(\mathbb{Z}_2)$ and $M_2(\mathbb{Z}_3)$.

If we restrict the inputs of the equivalence problem to monomials, then we are working in the multiplicative semigroup of the ring R. In this paper we examine the complexity of the equivalence problem over matrix semigroups, and it turns out that it has the same complexity as the equivalence problem for sum of monomials for the matrix rings. Our second result is the following:

Theorem 2. *For a matrix semigroup the equivalence problem is in P if the semigroup is commutative and coNP-complete, otherwise.*

For groups the characterization of the equivalence problem is far less complete. In 2004 Burris and Lawrence [2] proved that if G is nilpotent or $G \simeq D_n$, the dihedral group for odd n-s, then the equivalence problem for G is in P. Towards the hard side Horváth, Lawrence, Mérai and Szabó [4] proved, that for a non-solvable group G the equivalence problem is coNP-complete.

2. Preliminaries

Let $M_n(q)$ denote the ring of n by n matrices over the $q = p^\beta$ element field, $\mathbb{F}_q$. The *general linear group* $GL_n(q)$ is the group of invertible elements of $M_n(q)$, and the *special linear group*, $SL_n(q)$ is the subgroup containing the elements of determinant 1. All normal subgroups of $SL_n(q)$ are contained in its center, $Z(SL_n(q))$. The *projective linear group* $PSL_n(q)$ is defined as the factor of $SL_n(q)$ by $Z(SL_n(q))$. If $n > 2$ or $q > 3$, then $PSL_n(q)$ is simple.

The proof of Theorem 2 is a reduction to the equivalence problem to its group of units. Firstly, we focus on properties of matrix groups, and then show how our reduction works.

2.1. **Verbal Subgroups.** We start with some definitions and easy observations about verbal subgroups of groups and commutators using the terminology and notation of [4].

A subgroup H of a group G is a *verbal subgroup*, if it is generated by the ranges of a set of group terms T that is if $H = \langle \cup_{t\in T} t^G(G)\rangle$. Note that verbal subgroups are normal. Obviously $\{id\}$ and G are verbal subgroups of any group. If $\{id\}$ and G are the only verbal subgroups of G then G is called *verbally simple*. For a group G let d_G be the smallest positive integer such that for any set X of generators of G we have $G = \cup_{0\le k\le d_G} X^k$. Given a term $t(x_1, \dots, x_m)$, define the term t_d by

$$t_d\big(x_1, \dots, x_{md}\big) := \underbrace{t(x_1, \dots, x_m) \cdot t(x_{m+1}, \dots, x_{2m}) \cdots}_{\text{a product of } d \text{ terms } t(\cdots), \text{ with distinct variables}}$$

Note, that for a finite group G a verbal subgroup can always be expressed as a range of a single term. Indeed, for $T = \{t_1, \dots, t_k\}$ let $t = t_1 \cdots t_k$. Then $\langle \cup_{t\in T} t^G(G)\rangle = t_d^G(G)$ for any $d \geq d_G$.

The *commutator* is a group term defined by $c(x, y) = [x, y] := x^{-1}y^{-1}xy$. For $a \in G$ let $[a, G] := \big\langle \big\{ [a, g] : g \in G \big\} \big\rangle$. $[a, G]$ is a normal subgroup of G. If G is a non-abelian simple group then

$$[a, G] = \begin{cases} id & \text{if } a = id \\ G & \text{if } a \neq id. \end{cases}$$

If $n > 2$ or $q > 3$, the commutator subgroup of $GL_n(q)$ is $SL_n(q)$ and

$$[a, GL_n(q)] = \begin{cases} id & \text{if } a \in Z(GL_n(q)) \\ SL_n(q) & \text{if } a \neq id. \end{cases}$$

Our starting point will be the following result form [4].

Lemma 3. *For every graph, Γ and integer d there is a group term t such that*

(a) *for every group G the image of the term is contained in the commutator subgroup, $t(G) \lhd G'$*
(b) *if Γ is not $|G|$ colorable then $t(G) = \{id\}$.*
(c) *If G is a simple group and $d \geq d_G$, then $G \models t_d \approx id$ if and only if Γ is not $|G|$ colorable and $t_d(G) = G$ otherwise. Note that d is a parameter of the term t and so a double parameter of the term t_d.*
(d) *t (and t_d) can be constructed in polynomial time in the size of Γ.*

Now we are able to make the first step towards the reduction.

Theorem 4. *Let p be a prime, $q = p^\beta$, $q_1 = p^{\alpha_1}, \dots, q_m = p^{\alpha_m}$.*

(1) *Let $n > 2$ or $q > 3$ and $k = |PSL_n(q)|$. Then for every graph Γ and for every $d \geq d_{GL_n(q)}$ there is a group term t such that:*
   - *$GL_n(q) \models t_d \approx id$ if Γ is not k colorable and*
   - *$t_d(GL_n(q)) = SL_n(q)$ otherwise;*
   - *t can be constructed in polynomial time in the size of Γ.*

   Note that, as before, d is a parameter of the term t and so a double parameter of the term t_d.
(2) *Let $GL_{n_i}(q_i), \dots, GL_{n_m}(q_m)$ be matrix groups. Suppose, that $n_i > 2$ or $q_i > 3$ for all $1 \leq i \leq m$. And let $k = \max_{1\leq i\leq m}\{|PSLn_i(p^{\alpha_i})|\}$. Then for every graph Γ there is a group word u such that*
   - *if Γ is not k colorable then $GL_{n_i}(q_i) \models u \approx id$ for every i;*
   - *if Γ is k colorable then $u(GL_{n_i}(q_i)) = SL_{n_i}(q_i)$ for some $1 \leq i \leq m$.*

- *u can be constructed in polynomial time in the size of Γ.*

Proof of item 1. Let Γ be a graph. We show that t, the term constructed in Lemma 3 with any $d \geq d_G$ will do. Suppose that Γ is k colorable. Then we claim that $t_d(GL_n(q)) = SL_n(q)$ holds for $d \geq d_{GL_n(q)}$. By Lemma 3 $t_d(GL_n(q)) \lhd GL_n(q)' = SL_n(q)$. As $PSL_n(q)$ is simple, $t_d(PSL_n(q)) = PSL_n(q)$, hence the image of t over $SL_n(q)$ is not contained in the center of $SL_n(q)$. The subgroup $t_d(GL_n(q))$ is normal in $GL_n(q)$, so $t_d(GL_n(q)) = SL_n(q)$.

If Γ is not k colorable, then, again by Lemma 3, $t_d(GL_n(q)) = \{id\}$. Thus t satisfies the conditions of the lemma. □

Proof of item 2. Now, for item 2, let Γ be a graph and let t be the term constructed in Lemma 3 with $d = \max_i\{d_{GL_{n_i}(q_i)}\}$. Now, for every i we have $t_d(GL_{n_i}(q_i)) = SL_{n_i}(q_i)$ if Γ is not $|PSL_{n_i}(q_i)|$ colorable and $t_d(GL_{n_i}(q_i)) = \{id\}$, otherwise. Let us assume that Γ is not k-colorable. Then Γ is not l-colorable for any $l \leq k$. Thus $t_d(GL_{n_i}(q_i)) = \{id\}$ for every $1 \leq i \leq m$. Now, assume that Γ is k-colorable. Then $t_d(GL_{n_j}(q_j)) = SL_{n_j}(q_j)$ whenever $|PSLn_j(p^{\alpha_j})| = k = \max_{1\leq i\leq m}\{|PSLn_i(p^{\alpha_i})|\}$. Thus $u = t_d$ satisfies the conditions. □

2.2. **Matrix Semigroups.** For every matrix ring we will present an integer N such that for almost all matrices, A – except for a few invertible matrices – A^N is idempotent. The sizes of the groups $GL_m(q)$ and $SL_m(q)$ for $q = p^\beta$ are given by the following wellknown formulas.

$$\begin{aligned} |GL_m(p^\beta)| &= (p^{\beta m} - 1)(p^{\beta m} - p^\beta)\cdots(p^{\beta m} - p^{\beta(m-1)}) \\ &= p^{\beta\frac{m(m-1)}{2}}(p^{\beta m} - 1)(p^{\beta(m-1)} - 1)\cdots(p^\beta - 1) \end{aligned}$$

and

$$|SL_m(p^\beta)| = \frac{|GL_m(p^\beta)|}{p^\beta - 1}$$

Our main lead will be the following theorem of K. Zsigmondy ([10]).

Theorem 5. *Let a, k be integers greater than 1. Then except in the cases $k = 2$, $a = 2^\gamma - 1$ and $k = 6$, $a = 2$, there is a prime r with the following properties*

1. *r divides $a^k - 1$.*
2. *r does not divide $a^i - 1$, whenever $0 < i < k$.*
3. *r does not divide k.*

In particular, k is the order of a modulo r.

Lemma 6. *Let $M_n(q)$ be a matrix ring where $n > 1$ and $q = p^\alpha$. There is a positive integer N such that: for every $A \in M_n(q)$ either A^N is*

idempotent (a projection) or A^N is invertible in $M_n(q)$. Moreover there is at least one element in $B \in SL_n(q)$, such that $B^N \neq id$.

Proof. Case 1. Let $q = p^\alpha$ not among the exceptional cases of Zsigmondy's theorem. Then there is a prime r satisfying the requirements of Zsigmondy's theorem for $a = q^n$. Define k such that $r^k | q^\alpha - 1$ and $r^{k+1} \nmid q^\alpha - 1$, and let $N = \alpha \frac{|GL_\alpha(q)|}{r^k}$. Let A be an arbitrary matrix in $M_n(q)$. For every $m \geq n$ the matrix A^m acts on $W = \mathrm{Im}(A^m)$ as a linear transformation and the action is invertible. Thus if $\dim(W) = l$, then $(A^m)^{|GL_l(q)|}$ a projection (idempotent). Obviously,

- $\alpha \geq n$ and
- $|GL_l(q)|$ divides $|GL_n(q)|$ for every $n > l$, and
- $(r, |GL_l(q)|) = 1$ for every $n > l$.

Hence, if $l < n$, then $|GL_l(q)|$ divides $\frac{GL_n(q)|}{r^k}$. Thus for every matrix $A \in M_n(q)$, where A is not invertible, the matrix A^N is idempotent. Finally, r divides $|SL_n(q)| = \frac{|GL_n(q)|}{q-1}$. Thus by Cauchy's theorem there is an element $B \in SL_n(q)$ of order r. Clearly, $B^N \neq id$.

Case 2. Let $p = 2^{\gamma-1}$ and $n\alpha = 2$ then Then $N = 2(p-1)$ works.

Indeed, $|GL_1(p)| = p - 1$ and $|SL_2(p)| = \frac{(p^2-1)(p^2-p)}{p-1}$. Every nonzero, not invertible matrix $A \in M_2(p)$ is of rank 1. Thus $A^{2(p-1)}$ is a projection. If B is of order p (such an B exists by Cauchy's theorem), then, $B^{2(p-1)} = B^{p-2} \neq id$.

Case 3. Finally, let us consider the most unlucky case, where $q = 2$ and $n\alpha = 6$. The exponents of the appropriate groups are the following.

The exponents of $GL_m(2^\beta)$:

β \ m	1	2	3	4	5	6
1	1	6	84	420	26040	78120
2	3	30	1260			
3	7	126				

The exponents of $SL_m(2^\beta)$.

β \ m	1	2	3	4	5	6
1	1	6	84	420	26040	78120
2	1	30	420			
3	1	126				

Let A be an arbitrary matrix in $M_n(q)$. As in the previous two cases, for every $m \geq n$ the matrix A^m acts on $W = \mathrm{Im}(A^m)$ as a linear transformation and the action is invertible. Now, $11 \geq n$ in each case, and 11 relatively prime to the exponent of each group. Hence A^{11} acts invertible on its image and every invertible matrix in each of these

matrix rings is of the form A^{11}. So we need a number K such that $expSL_n(q) \nmid K$ and $expGL_l(q)|K$ for every $l < n$, and then $N = 11K$ will do. For $SL_2(6)$ we can choose $K = 26040$, for $SL_3(4)$ we can choose $K = 30$ and for $SL_2(8)$ we can choose $K = 7$.

□

Lemma 7. *Let $M_{n_1}(q_1), \ldots, M_{n_m}(q_m)$ be matrix rings, where $q_i = p^{\alpha_i}$ for a fixed prime p. Let $\alpha = \max\{n_i\alpha_i\}$. Then there is a polynomial $f(x)$ over the p-element field $\mathbb{F}_p$ such that for every $A \in M_{n_i}(q_i)$ with $n_i\alpha_i < \alpha$ the equation $f(A) = 0$ holds. Moreover, if $n_j\alpha_j = \alpha$, then and there is a matrix in $C \in SL_{n_j}(q_j)$ such that $f(C) \in GL_{n_j}(q_j)$.*

Proof. Let $g \in \mathbb{F}_{p^\alpha}$ be a field element of degree α with norm 1 over $\mathbb{F}_{q_j}$.

Such an element exists by Hibert's Theorem 90. E.g. if h is a generator of the multiplicative group of $\mathbb{F}^*_{p^\alpha}$ that is $\langle h\rangle = \mathbb{F}^*_{p^\alpha}$, then $g = h^{1-q_j}$ works. The norm of the element in this case is the constant term of its minimal polynomial.

Let $m(x)$ be the minimal polynomial of g over $\mathbb{F}_p$. Let $C \in M_{n_j}(q_j)$ be a matrix with minimal polynomial $m(x)$ (over $\mathbb{F}_p$). Now as $\det(C)$ is the norm of g, the determinant of C is equal to 1, $C \in SL_{n_j}(q_j)$ and its minimal polynomial $m(x)$ is irreducible over $\mathbb{F}_p$ of degree $n_j\alpha_j = \alpha$. Let $g(x)$ be the least common multiple of all polynomials of degree at most α and let $f(x) = \frac{g(x)}{m(x)}$. Now $(m(x), f(x)) = 1$, hence $f(C) \in GL_{n_j}(q_j)$. Let $A \in M_{n_i}(q_i)$ for some i with $n_i\alpha_i < \alpha$ $m_A(x)$ its minimal polynomial over $\mathbb{F}_p$. The degree of $m_A(x)$ is less then α, hence $m_A(x)|f(x)$ and $f(A) = 0$ as we wanted. □

3. The Equivalence Problem for Rings

Proof of Theorem 2 . For $M_2(\mathbb{Z}_2)$ and $M_2(\mathbb{Z}_3)$ the theorem was proved in [8] and [9]. Let $n > 2$ or $q > 3$. We reduce the equivalence problem of $M_n(\mathbb{F})$ to graph k-coloring where $k = |PSL_n(q)|$. Let Γ be a graph. By Theorem 4 there is a group term s (of polynomial length in the size of Γ) such that $s \approx id$ over $GL_n(q)$ if and only if Γ is not k-colorable and if $s \not\approx id$ then $s(GL_n(q)) = SL_n(q)$. Let us substitute $x^{|GL_n(q)|-1}$ for every occurrence of the inverse of the variable x to obtain a semigroup word, t. The terms t and s are equivalent over the (semi)group $GL_n(q)$. The length of t is at most $|GL_n(q)| - 1$ times the length of s, hence polynomial in the size of Γ. Let N be the integer chosen in Lemma 6. We claim that $t \approx id$ over the (semi)group $GL_n(q)$ if and only if $t^{2N} \approx t^N$ over the semigroup $M_n(q)$. For a non invertible matrix A the identity $A^N = A^{2N}$ holds by assumption, hence $t^{2N} \approx t^N$ over $M_n(q)$ if and only if $t^{2N} \approx t^N$ over $GL_n(q)$. If $t \approx id$, then $t^{2N} \approx t^N$ obviously holds. Let

us assume that $t \not\approx id$. Then $t(GL_n(q)) = SL_n(q)$ and by Lemma 6 there is an $B \in SL_n(q)$, such that $B^N \neq id$, hence $t^{2N} \not\approx t^N$. Thus $t \approx id$ if and only if Γ is k-colorable, and the equivalence problem for the semigroup $M_n(q)$ is coNP-complete. □

Proof of Theorem 1. Item (1) is proved in [6].

For part (2) let n denote the nilpotency class of $J(R)$. It is the least integer such that $J(R)^n = 0$. The factor ring $R/J(R)$ is a direct sum of matrix rings over finite fields, say $R/J(R) = M_{n_1}(p_1^{\alpha_1}) \oplus M_{n_2}(p_2^{\alpha_2}) \oplus \cdots \oplus M_{n_m}(p_m^{\alpha_m})$. Let $p = p_i$ be a prime such that $n_i > 1$. Let P denote the product of all primes occurring amongst $\{p_1, p_2, \ldots, p_m\}$ distinct from p_i. Let $q_i = p_i^{\alpha_i}$ and $M_{n_1}(q_1)$, $M_{n_2}(q_2), \ldots M_{n_l}(q_l)$ be the matrix rings with characteristic p. Let s be the term constructed in Lemma 4, item 2 for the groups $GL_{n_1}(q_1), \ldots, GL_{n_l}(q_l)$, let $f(x)$ be the polynomial from Lemma 7 for $M_{n_1}(q_1), \ldots, M_{n_l}(q_l)$ and let $\alpha = \max\{n_i\alpha_i \mid i = 1, 2, \ldots, l\}$.

So, the following hold for the number P, semigroup term s and polynomial f:

- $P \cdot M_{n_i}(q_i) = \begin{cases} M_{n_i}(q_i) & \text{if } q_i = p^{\alpha_i} \text{ and} \\ 0 & \text{otherwise .} \end{cases}$
- $s(GL_{n_i}(q_i)) = \begin{cases} SL_{n_i}(q_i) & \text{if } \Gamma \text{ is } k \text{ colorable and} \\ id & \text{otherwise .} \end{cases}$
- $f(C) \begin{cases} \neq id \in GL_{n_i}(q_i) \text{ for some } C \in SL_{n_i}(q_i) & \text{if } \alpha = n_i\alpha_i \\ = 0 & \text{otherwise.} \end{cases}$

Here, $Px = x + x + \cdots + x$, the addition is iterated P times.

Now, the polynomial $P \cdot f(s) \approx 0$ over $R/J(R)$ if and only if Γ is k-colorable. We check this identity coordinatewise. If $q_i \neq p^\beta$ for some β, then multiplying by P annihilates the ith coordinate. For $q = p^{\alpha_i}$ if Γ is not k-colorable, then $s(GL_{n_i}(q_i)) = 1$ for every i and every other value of s is not invertible. Thus $f(s(M_{n_i}(q_i))) = 0$. If Γ is k-colorable, then $s(GL_{n_i}(q_i)) = SL_{n_i}(q_i)$ for some i and so $f(s(M_{n_i}(q_i))) \neq 0$.

Finally, we claim that $R \models (P \cdot f(s))^n \approx 0$ if and only if $R/J(R) \models P \cdot f(s) \approx 0$. Indeed, if $R/J(R)P \cdot f(s) \approx 0$, then $P \cdot f(s)(R) \subseteq J(R)$, so $P \cdot f(s))^n \approx 0$ over R. If the identity $P \cdot f(s) \approx 0$ fails in $R/J(R)$, then there is an invertible matrix $C \in P \cdot f(s)(R/J(R))$. Obviously $C^n \neq 0$ in $R/J(R)$, thus $(P \cdot f(s))^n \approx 0$ fails in R, as well.

The length of s is polynomial in the size of Γ. The length of $f(x)$ and P depend only on R, and so the length of the term is polynomial in the size of Γ, when expanded as a sum of monomials. □

4. Acknowledgements

The research of the authors was supported by the Hungarian National Foundation for Scientific Research, Grants N67867 and K67870.

References

[1] S. Burris and J. Lawrence. The equivalence problem for finite rings. *Journal of Symbolic Computation*, 15:67–71, 1993.
[2] S. Burris and J. Lawrence. Results on the equivalence problem for finite groups. *Algebra Universalis*, 52(4):495–500, 2004.
[3] M. Goldmann and A. Russel. The complexity of solving equations over finite groups.
[4] G. Horváth, J. Lawrence, L. Mérai, and Cs. Szabó. The complexity of checking identities in non-solvable groups. *Bull. Lond. Math. Soc.*, 2006, to appear.
[5] H. Hunt and R. Stearns. The complexity for equivalence for commutative rings. *Journal of Symbolic Computation*, 10:411–436, 1990.
[6] J. Lawrence and R. Willard. The complexity of solving polynomial equations over finite rings. manuscript, 1997.
[7] V. Yu. Popov and M. V. Volkov. Complexity of checking identities and quasi-identities in finite semigroups. *Journal of Symblic logic*, to appear.
[8] Cs. Szabó and V. Vértesi. The complexity of the checking identities for finite matrix rings. *Algebra Universalis*, (51):439–445, 2004.
[9] Cs. Szabó and V. Vértesi. The complexity of the word-problem for finite matrix rings. *AMS Proceedings*, (132):3689–3695, 2004.
[10] Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* , (3):265–284, 1892.

Eötvös Loránd University, Department of Algebra and Number Theory, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary
E-mail address: csaba@cs.elte.hu
E-mail address: wera13@cs.elte.hu